Common Criteria

Evaluation and Validation Scheme

for

Information Technology Security

Guidance to Sponsors of IT Security Evaluations

Scheme Publication #5

DRAFT

Version 1.0

31 August 2000

Please submit comments to scheme-comments@nist.gov

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Systems Security Organization
9800 Savage Road
Fort George G. Meade, MD 20755

Table of Contents

1 Introduction

The Common Criteria Evaluation and Validation Scheme (CCEVS) was established by the National Information Assurance Partnership (NIAP). NIAP is a partnership established by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to evaluate conformance of Information Technology (IT) products/systems and specifications (protection profiles) to international standards. The principal participants in the program are the Sponsors of IT product/system or protection profile evaluations, the product/system or protection profile developer, the Common Criteria Testing Laboratories (CCTLs), and the CCEVS Validation Body.

A Sponsor is the party requesting the security evaluation of an IT product/system or protection profile (PP). The sponsor may be the developer of a PP, the developer of an IT product/system, a value-added reseller of an IT product/system, or another party that wishes to have an IT product/system or PP evaluated.

A CCTL is a commercial testing laboratory accredited by the National Voluntary Laboratory Accreditation Program (NVLAP). CCTLs are approved by the CCEVS Validation Body to perform security evaluations against the Common Criteria for Information Technology Security Evaluation (CC) using the *Common Methodology for Information Technology Security Evaluation* (CEM).

The CCEVS Validation Body, hereafter referred to as the Validation Body, is the government organization established by the NIAP to implement and operate the validation scheme for the U.S. Government. This document, the fifth in a series of CCEVS publications, provides guidance to sponsors of IT product/system or PP evaluations.

NIST and NSA have the following objectives in developing, operating, and maintaining an evaluation and validation scheme:

a) meet the needs of government and industry for cost-effective IT evaluations,

b) encourage the formation of commercial security testing laboratories and the development of a private sector security testing industry,

c) ensure that security evaluations of IT products are performed to consistent standards,

d) improve the availability of evaluated IT products, and

e) facilitate the use of evaluation as an effective and efficient part of an overall strategy for improving the trustworthiness of U.S. information technology.

The scheme is intended to serve many communities of interest with very diverse roles and responsibilities. These communities include IT product developers, product vendors, value-added resellers, systems integrators, IT security researchers, acquisition/procurement authorities, consumers of IT products, auditors, and accreditors (individuals deciding the fitness for operation of those products within their respective organizations). Close cooperation between government and industry is paramount to the success of the scheme and the realization of its objectives.

1.1 Purpose

This document provides guidance to the sponsor of an IT product/system or PP evaluation under the CCEVS. It will help the sponsor prepare for and understand his roles prior to, during, and after an IT product/system or PP evaluation. This document will help the sponsor understand and use the CCEVS validation services. It expands upon the requirements stated in Annex D of Scheme Publication #1*, NIAP Common Criteria Evaluation and Validation Scheme for IT Security -- Organization, Management and Concept of Operations*. The specific obligations of the sponsor of an evaluation are outlined in this document. Additionally, what the sponsor can expect of the CCTL and the Validation Body is identified.

The primary audience of this document is the sponsor of IT product/systems or PP evaluations. Others who may find it useful include the CCTL staff, security target (ST) and protection profile (PP) authors, product developers, and CCEVS Validation Body staff.

1.2 Definition of Sponsor

The *sponsor* is the individual or organization requesting a security evaluation of an IT product/system or a protection profile. The relationship of the sponsor to the IT product/system or protection profile may vary depending on the nature of the product or profile and the circumstances surrounding the evaluation. In most cases, the sponsor of a security evaluation will be the actual developer of the IT product/system or protection profile. However, this may not always be the case. The sponsor of a security evaluation may be a value-added reseller of an IT product/system or an organization or individual involved in the acquisition of an IT system that includes that particular product as an essential component. The sponsor may also be an independent contractor, serving as a systems developer or integrator attempting to fulfill the requirements of a contract. Consortia or trade associations may nominate a single point of contact to serve as the sponsor of an evaluation.

When the sponsor of an evaluation is not the developer of the product or PP, the sponsor must work cooperatively with the developer. Regardless of whether or not the sponsor is the developer, the CCTL must be provided with the technical materials and essential deliverables needed to conduct the IT security evaluation in a complete and consistent manner. The details of the provision of materials for the security evaluation will be handled in contractual agreements between the sponsor and the developer.

1.3 Organization of this Document

This document consists of four chapters and several supporting annexes. Chapter 1 provides an introduction, defines the purpose of the document, gives the definition of 'Sponsor', and identifies additional sources of information. Chapter 2 provides an overview of the CCEVS evaluation process and gives a description of the major elements of a CC evaluation. Chapter 3 provides a description of the services and assistance that is available from the CCEVS Validation Body. Chapter 4 provides guidance to sponsors of CC evaluations for each phase of the evaluation: pre-evaluation, evaluation, and post-evaluation.

The supporting annexes cover a variety of topics, including the following:

Annex A – Demonstrating CC Conformance (approaches that the sponsor may use for demonstrating to consumers the conformance of a PP or IT product to the Common Criteria),

Annex B – Web sites that provide useful information to sponsors and that are referred to throughout the document,

Annex C – Sample Evaluation Acceptance and Non-Disclosure Agreement,

Annex D – Acronyms used in this document.

1.4 Other CCEVS Sources for Sponsor Information

Additional sponsor-related information can be found in:

a. Scheme Publication #1 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security -- Organization, Management, and Concept of Operations,*

b. Scheme Publication #2 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security -- Validation Body Standard Operating Procedures,*

c. Scheme Publication #3 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security -- Technical Oversight and Validation Procedures,*

d. Scheme Publication #4 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security -- Guidance to Common Criteria Testing Laboratories,*

e. Scheme Publication #6 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security -- Certificate Maintenance Program, and*

f. CCEVS Bulletins and Newsletters.

Copies of all scheme publications, Guidance Documents, and other important information about the CC, CCEVS Validation Body, commercial testing laboratories, and validated IT products are available on the CCEVS web site at **http://niap.nist.gov/cc-scheme**.

2 Common Criteria Evaluation Overview

Consumers of IT products need to have confidence in the security features of those products. Consumers want to be able to compare various products to understand their capabilities and limitations. Confidence in a particular IT product can be based on the trusted reputation of the developer, past experience in dealing with the developer, or the demonstrated competence of the developer in building products through recognized assessments.

The Common Criteria Scheme provides consumers with an impartial assessment of an IT product by an independent entity. This impartial assessment includes an analysis of the IT product and the testing of the product for conformance to a set of security requirements. IT security evaluations are composed of analysis and testing, distinguishing these activities from the more traditional forms of conformance testing in other areas.

The Common Criteria (CC) is a catalog of security requirements. This catalog is used as the source for building requirement sets that form the basis for IT security evaluations. The application of the CC is expressed through the following documents:

- Protection Profile (PP)
- Target of Evaluation (TOE)
- Security Target (ST)
- Common Evaluation Methodology (CEM)

2.1 Protection Profile (PP)

The CC defines a PP as an implementation independent set of security requirements for a category of IT products, which meet specific consumer needs.

The PP is essentially a system design document that starts with a statement of need and refines it though several levels to a solution that meets the need. It is not just a set of requirements but a framework for defining requirements that shows what is addressed and gives the context for relating the requirement set to a specific user's needs.

A protection profile:

- identifies the security capability to be provided,

- describes the IT portion of the solution that is the subject of this requirement set,
- describes the environment in which the security issues are to be addressed,
- gives the security objectives that, when met, will provide the identified security capability,
- specifies the security requirements (function and assurance) needed to accomplish this, and
- provides a rationale showing the specified requirements do in fact provide the identified security capability.

2.2 Target of Evaluation (TOE)

The target of evaluation (TOE) is an IT product or group of IT products configured as an IT system and associated documentation that is the subject of a security evaluation under the Common Criteria.

The TOE is the IT product/system that is the subject of the requirement set being specified by the PP (or the security target described below). Additionally, the TOE is the security-related user and administrator guidance associated with the IT product/system.

2.3 Security Target (ST)

While the PP is implementation independent, a security target (ST) is a specification of the security required (both functionality and assurance) in a Target of Evaluation (TOE), used as a baseline for evaluation under the Common Criteria.

The ST, like a PP, specifies:

- the security capability to be provided,
- the environment in which this capability is to be provided,
- the security objectives that, when met, will provide the needed capability in the specified environment, and
- the specific security requirements (functional and assurance) needed to accomplish this.

In addition, the ST identifies the specific security mechanisms that will be employed, and indicates the PP(s), if any, with which the ST is compliant.

The ST does not need to be derived from a PP. The ST can stand alone – perhaps describing the security characteristics of existing IT product/system. Whether developed in response to a PP (which is essentially a statement of user need like a request for proposal), or developed separately, the ST construct provides a common format for describing security requirements. The ST, unlike previous requirement sets and most existing vendor produced product descriptions, gives context for the requirements and provides a rationale for why the requirements implement the claimed capabilities.

2.4 Common Evaluation Methodology (CEM)

In order for evaluations conducted in different testing laboratories to meet a common set of expectations, a standard evaluation methodology is needed. This is provided by the CEM. The CEM provides, for each assurance component (currently those used in EAL 1-4), a specified set of work-units to be performed. Along with each work-unit is text describing the nature of the work to be performed. In addition, the CEM gives guidance for a number of evaluation areas (e.g., the selection of subsets of evidence for evaluator actions).

3 Validation Body Assistance and Services

The CCEVS provides both assistance and services to customers. Assistance provided by the Validation Body is generally limited to: responding to questions by phone; holding/attending informational meetings; conducting workshops; providing educational courses; providing the latest information on Scheme processes, procedures, and CC/CEM interpretations; and providing guidance on the type of evidence required for an evaluation. Validation Body services consist of work performed for customers under an agreed upon work plan or statement of work. The CCEVS does not provide services for preparing sponsor material for the evaluation or in the collection or preparation of CC/CEM evidence.

Usually, CCEVS assistance is provided without charge. However, in cases where the Validation Body may incur extended costs, (for workshops, classes, travel, etc.) the sponsor may be required to reimburse the Validation Body for expenses incurred.

3.1 CCEVS Assistance Priorities

The Validation Body intends to quickly respond to sponsors' requests for assistance/information. In the event that there are multiple requests competing for CCEVS resources that cannot immediately be responded to, the Validation Body will focus its resources in the following priority order:

a. Active validation projects that have been formally accepted into the Scheme,
b. Maintenance of current validation certificates,

c. Requests pertaining to future validations responding to Federal procurement actions,
d. Requests pertaining to future validations that are not subject to Federal procurement actions.

3.2 NIAP CCEVS Educational Courses

Courses are available through NIAP that provide a background in the Common Criteria. Specifically, there is a one-day CC introductory course (Class #1), a four-day course in developing a Protection Profile (Class #2), and a one-week course on the Common Evaluation Methodology. These courses are open to the public. Additional information and a course schedule can be found at http://www.niap.nist.gov/event.html#Classes.

3.3 Answers to Scheme Questions

Prior to the start of the evaluation, potential sponsors may have questions about the Scheme.

Prior to submitting a request for CCEVS procedure guidance, the sponsor should review the NIAP CCEVS Guidance Publications or Frequently Asked Questions (FAQ) to see if these sources provide the answers needed. The CCEVS web site containing this information is http://niap.nist.gov/cc-scheme/GuidanceDocs.html

3.4 Requests for CC and CEM Interpretation

A common request is for interpretation of the CC or the CEM. The Validation Body will entertain any question at any time and will make every effort to provide a timely response. The Validation Body is prepared to respond to general questions by telephone or in meetings. However, the required method for submitting specific questions about criteria interpretation is in writing (by letter or email). The Validation Body will provide a written response to all requests for interpretation.

Before submitting a request for criteria interpretation, the sponsor should:

1. Review the Common Criteria Interpretation Management Board's (CCIMB) current list of interpretations to see if the current available interpretations provide the necessary answers. The web site for the CCIMB is located at http://www.commoncriteria.org/

2. Review any CCEVS interim interpretations not covered by the CCIMB interpretations to determine if these provide the necessary information. The web site for the CCEVS interpretations is http://niap.nist.gov/cc-scheme/.

After the two steps above have been followed, further criteria interpretation questions may be directed to the Director of the CCEVS.

3.5 Validation Services

The primary focus of the CCEVS work is to provide validation services to CCTLs and sponsors. Validation services are the activities followed in assuring that a given PP or IT product/system evaluation has been conducted in accordance with the provisions of the NIAP CCEVS, CC, CEM and CCRA; ensuring that the results of the IT security evaluations produced by the CCTLs are validated; and when all the required CCEVS conditions have been met, issuing a Common Criteria Certificate on the PP or IT product/system. The specific validation activities to be performed by the Validation Body for a PP or IT product/system evaluation are defined in the Validation Body work plan for the PP or IT product/system evaluation.

The Validation Body will provide validation services for sponsors and CCTLs at no charge during the initial two-year period of CCEVS operation. The actual cost of these services, to include technical oversight and monitoring, final issuance of Common Criteria certificate, publication of validation reports, and the posting of IT products and protection profiles on the NIAP Validated products List will be monitored and assessed during the initial period of CCEVS operation. The Validation Body intends to initiate a cost-recovery program for validation services after the initial two-year period.

4 Sponsor Guidance

This section provides guidance that is relevant to sponsors prior to starting an evaluation, during an evaluation, and after the completion of an evaluation.

The period of *pre-evaluation* is considered to be any activity that occurs pertinent to an evaluation/validation before the signing of legal agreements between the sponsor/CCTL /Validation Body for acceptance of the evaluation as a scheme project.

An *evaluation* commences once the legal agreements are signed and ends just prior to the issuance of the Validated Products List entry.

Post-evaluation commences with the issuance of the certificate and the publication of the Validated Products List entry.

4.1 Pre-Evaluation

The primary sponsor responsibility during the pre-evaluation phase is to obtain sufficient information in order to prepare for the CC evaluation and validation process. Information may be gathered from a variety of sources, including consulting with a CCTL or other company, open source literature, and contacting the Validation Body. The sponsor is also responsible for providing the required material for the CC evaluation, and securing the appropriate legal and non-disclosure agreements.

4.1.1 Selecting a CCTL

The list of accredited CCTLs is located at http://niap.nist.gov/cc-scheme/TestingLabs.html. When selecting a CCTL for consulting prior to an evaluation, or for performing the evaluation, or both, the sponsor should use a careful screening process. The experience of the CCTL personnel with both the technology and the target Evaluation Assurance Level (EAL), the fees, the estimated schedule, and any other pertinent factors should be reviewed and considered before the sponsor enters into a contractual relationship with a CCTL. Details of the contract between the CCTL and the sponsor are left to the two parties to negotiate, with no involvement by the Validation Body.

4.1.2 Consulting with a CCTL in Support of Evaluation

It is important to note that there must be no apparent or perceived conflict of interest between those individuals performing consulting services for an evaluation and the evaluation team personnel. Specifically, there must be a clear and definite separation of personnel between these two functions. If a CCTL is used for both consulting and evaluation, contract negotiations between the CCTL and the sponsor should clearly specify that different personnel must be used for the two different functions.

The scope of consulting work during the preparation for an IT security evaluation is not controlled by the scheme and is a matter of negotiation between the sponsor and the CCTL or other consultant. However, the CCTL must adhere to the terms and conditions of its NVLAP accreditation to ensure that the advice given does not affect evaluator independence or impartiality in any evaluation.

4.1.3 Preparation for IT Security Evaluation

The majority of activity in the early stages of an evaluation occurs between the sponsor of the evaluation and the CCTL. The sponsor is responsible for providing the protection profile (PP) or the security target (ST) and the associated IT product/system that will become the Target of Evaluation (TOE). The composition of a TOE may vary and may consist of hardware, firmware, and software (or any combination thereof). The TOE may also include multiple IT products (sometimes referred to as an IT system), some of which may already be evaluated. The sponsor must ensure that arrangements have been made to provide all essential documentation to the CCTL evaluation team in order to conduct a successful security evaluation.

4.1.4 Evaluation Assurance Levels (EALs) 5 through 7

Currently, the major scope of the CEM and CCEVS procedures and guidelines focuses on evaluating information technology products and protection profiles against the *Common Criteria for Information Technology Security Evaluation* (CC) at Evaluation Assurance Levels (EAL) 1 through 4. Because there is little agreed upon CEM guidance for Evaluations/Validations above EAL 4 the current Common Criteria Recognition Agreement (CCRA) only provides mutual recognition of evaluations/validations at EAL 1 through 4. Evaluation/validations at EAL 5 and above are currently not recognized under the CCRA.

Nevertheless, sponsors and CCTLs are encouraged to work with the Validation Body in conducting evaluations/validations at EAL 5 and above. The Validation Body will work with sponsors and CCTLs on a case-by-case basis in assessing those CC components above EAL 4. Depending on the technology and the circumstances, the U.S. Government may opt to have Government Evaluators accomplish the tasks and provide the results to the CCTL, may choose to augment CCTL's team with Government Evaluators, may provide supplemental evaluation methodology and have the CCTL conduct the evaluation, or any combination of the above.

Successfully completed evaluations/validations at EAL5-7 will be posted to the VPL with the caveat that some components are above EAL4 and therefore are beyond the scope of the CCRA.

4.1.5 Deliverables

4.1.5.1 Protection Profile and Security Target Deliverables

For an evaluation of a Protection Profile (PP), the PP itself is the deliverable to be provided by the sponsor.

An IT product or system evaluation requires the development and delivery of a Security Target (ST).

The security target serves as both a specification of the security functions against which the IT product (i.e., TOE) will be evaluated and as a description relating the product to the environment in which it will operate. The ST includes a list of claims about the IT product/system that are made by the sponsor, one of which may be conformance to a PP. The deliverables for a ST evaluation are the ST itself and any PPs to which the ST claims compliance.

4.1.5.2 Sources and Guidance for Producing STs and PPs

The content and presentation of both a PP and a ST must be specified in terms of the Common Criteria.

The development of a PP or ST can be a daunting task for those who are not experienced in writing such documents. Several sources exist to aid in developing PPs and STs. These sources are listed below.

a. Existing PPs and STs: Draft and final PPs are available on the Protection Profile Registry at web site http://csrc.nist.gov/cc/pp/pplist.htm. Security Targets are available with each CCEVS Validation Report. A list of validated products and associated CCEVS Validation Reports can be found on the scheme web site at http://niap.nist.gov/cc-scheme/ValidatedProducts.html. Electronic versions of the STs are typically found at the end of the CCEVS Validation Reports on the web site.

b. CC Toolbox: The Common Criteria Toolbox is a software application that automates the process of constructing PPs and STs. The CC Toolbox and associated documentation is freely distributed without charge. The web site for the CC Toolbox is http://niap.nist.gov/secrequire.html/CCToolbox.

c. Commercial Companies: Many of the CCTLs offer consulting services for helping vendors or sponsors develop PPs and STs. Security engineering firms or consultants well versed in the Common Criteria are also potential sources of assistance. As noted earlier, there can be no appearance of bias or conflict of interest by those conducting evaluations. Therefore, the sponsor must ensure that the PP/ST consultants will have no involvement in the actual PP or IT product/system evaluation. The list of accredited CCTLs can be found at the following web site: http://niap.nist.gov/cc-scheme/TestingLabs.html.

d. ISO 15408 Common Criteria Standard: The Common Criteria for Information Technology Security Evaluation (CC), ISO 15408, defines the structure, presentation and content of both a PP and a ST. The CC also serves as a catalog of CC IT security functional and assurance requirements. The CC can be found on the web at: http://csrc.nist.gov/cc/ccv20/ccv2list.htm.

e. Guide for the Production of PPs and STs: This document provides guidance related to the construction of PPs and STs that are intended to be compliant with the CC. The document is currently in draft form and is available at http://csrc.nist.gov/cc/PP/PPList.htm#PPGUIDE.

f. Guidance for COTS Security Protection Profiles (CSPP, NISTIR 6462): This document provides NIST guidance on the production of PPs for near-term commercial-off-the-shelf information technology. The document can be found at: http://csrc.nist.gov/publications/nistir/index.html.

4.1.5.3 TOE Deliverables

The deliverables for the evaluation of a TOE against its ST are typically items of hardware, firmware, software, and technical documentation normally generated during the development of the product. Additional TOE security-relevant documentation must be developed and delivered as required by the assurances in the ST.

Appropriate contractual arrangements shall be made by the sponsor to ensure that evaluation deliverables are provided to the CCTL. If the TOE consists of multiple IT products, some of which have been previously evaluated, the sponsor of the evaluation must ensure that contractual arrangements include authority for the release of previous evaluation results if reuse of these results is desired.

4.1.6 Readiness for Evaluation

Once the sponsor has established the PP or ST and the strategy for the supply of deliverables, the sponsor should select a CCTL to conduct the evaluation of the PP or IT product/system. A sponsor may provide potential CCTLs with the completed PP or ST in order to obtain more accurate evaluation proposals.

The CCTL selected to conduct the evaluation should review the PP/ST to ensure that it provides a sound basis for the evaluation.[1] The sponsor should address any issues raised in the PP/ST prior to the start of the evaluation. When a successful evaluation seems feasible, the CCTL should prepare an *Evaluation Work Plan*, an *Evaluation Schedule*, and a *Deliverables List*.

4.1.7 Entering the Scheme (CCEVS)

Generally, the CCTL will contact the Validation Body to request formal acceptance of the evaluation into the scheme, although a sponsor may do so in

[1] This informal review of the security target by the CCTL should not be confused with the formal evaluation of the security target conducted by the laboratory in accordance with the requirements of the Common Criteria and Common Evaluation Methodology.

conjunction with the CCTL. The following written information is required by the Validation Body before accepting a prospective evaluation into the scheme:

a) evaluation work plan;

b) evaluation schedule;

c) the ST and description of the TOE (in the case of an IT product/system evaluation); OR

d) the PP (in the case of a PP evaluation).

The Validation Body reviews the documentation in order to assess readiness for evaluation. This initial review may include meetings with the sponsor and key personnel from the CCTL and it is intended to mitigate risk on behalf of all participants in the evaluation and validation processes. The specific activities associated with this review process are described in Scheme Publication #3, *NIAP Common Criteria Evaluation and Validation Scheme for Information Technology Security—Technical Oversight and Validation Procedures*.

Due to the technical oversight and validation activities required by the Validation Body in fulfillment of its obligations under the *Agreement on the Recognition of Common Criteria Certificates in the field of IT Security (CCRA)*, sponsors desiring mutually recognized evaluation results are advised against allowing any evaluation tasks to be started by the CCTL before the evaluation is formally accepted into the scheme.

Figure 4-1 summarizes the activities associated with preparation for evaluation.

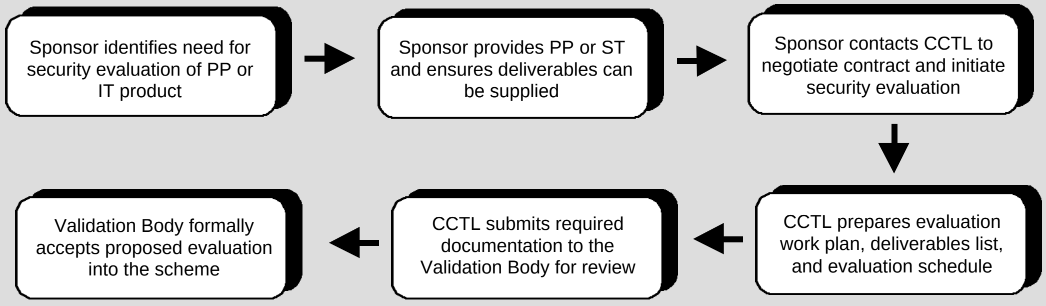

Sponsor identifies need for security evaluation of PP or IT product
Sponsor provides PP or ST and ensures deliverables can be supplied
Sponsor contacts CCTL to negotiate contract and initiate security evaluation
CCTL prepares evaluation work plan, deliverables list, and evaluation schedule
CCTL submits required documentation to the Validation Body for review
Validation Body formally accepts proposed evaluation into the scheme

Figure 4-1. Preparatory Activities for Security Evaluation

4.1.8 Proprietary/Sensitive Information

4.1.8.1 Access to Proprietary/Sensitive Information

The sponsor must ensure that the CCTL and the Validation Body are provided with all the PP or IT product/system related information and materials needed in order to complete the evaluation and validation process. Some of the required information for the evaluation/validation may be proprietary or sensitive. It is the sponsor's responsibility to fully and clearly identify the proprietary or sensitive information, to ensure all legal rights to the TOE and related material have been obtained, and to sign the appropriate non-disclosure agreement with the CCTL and Validation Body.

Before the Validation Body will accept an application to conduct a validation, the sponsor must sign a non-disclosure agreement. Annex C provides a sample non-disclosure agreement.

During the course of an evaluation/validation, information about the sponsor's PP or IT product/system may be shared between the CCTL and the Validation Body staff. No restrictions shall be placed on information shared between these organizations. As a condition of employment with the Validation Body, all employees must sign a Statement of Personal Responsibility for Non-Disclosure of Proprietary Information confirming their agreement to protect proprietary/sensitive information.

4.1.8.2 Public Information

As a condition of a validation, certain types of information are made available to the public. The Validation Report and the Validated Products List are examples of publicly available information. The sponsor must review and agree in writing to the posting of information before it is publicly posted. The sponsor must notify the Validation Body in writing when entering into a validation agreement if the sponsor does not wish to have a validation report or validated product listed on the Validated Products List (e.g., because it is procurement sensitive).

Any requests to the Validation Body for information about the sponsor's product or evaluation/validation that involve information beyond that which is publicly available will be referred to the sponsor.

4.1.9 Sponsor Responsibilities

Prior to the start of the evaluation, the sponsor is expected to:

a) enact a contract with the CCTL for the conduct of the evaluation, making clear the nature of the evaluation.

b) coordinate with the CCTL to produce an agreed upon evaluation work plan and schedule

c) commit to the CCTL to fulfill the sponsor role.

PP evaluation:

During pre-evaluation of a PP, it is the responsibility of the sponsor to:

a) determine the PP;

b) secure all legal rights to the PP and to indemnify the CCTL and Validation Body in this area;

c) ensure that the CCTL submits and gains acceptance of the evaluation into the scheme;

d) ensure that the CCTL submits a copy of all required documentation to the Validation Body;

e) meet all requests from the Validation Body for information and support during evaluation and validation;

f) agree not to make any statements in press releases or any other promotional material that might misrepresent the conclusions of the evaluation and validation or might otherwise bring the scheme into disrepute; and

g) attend meetings with the CCTL and the Validation Body, as required.

IT Product/system evaluation:

During pre-evaluation of an IT product/system, it is the responsibility of the sponsor to:

a) determine the ST for the evaluation and any PPs that the ST will attempt to satisfy;

b) secure all legal rights to the TOE and other deliverables necessary to conduct the evaluation and to indemnify the CCTL and Validation Body in this area;

c) provide to the Validation Body with written confirmation of the nature and extent of proprietary information associated with the TOE;

d) obtain the written consent of the IT product developer regarding the conditions for limiting access to proprietary information associated with the TOE;

e) ensure that the CCTL submits and gains acceptance of the evaluation into the scheme;

f) ensure that the CCTL submits a copy of all required documentation to the Validation Body;

g) meet all requests from the Validation Body for information and support during evaluation and validation;

h) give permission for the future release of evaluation results including extracts from evaluation technical reports that are relevant to Common Criteria certificate maintenance activities;

i) state whether the TOE's Common Criteria certificate is to be maintained under the Certificate Maintenance Program, and if so, to specify in the ST and assurance maintenance plan, the requirements for re-evaluation and maintenance of the certificate;

j) agree not to make any statements in press releases or any other promotional material that might misrepresent the conclusions of the evaluation and validation or might otherwise bring the scheme into disrepute; and

k) attend meetings with the CCTL and the Validation Body, as required.

4.1.10 Sponsor's Expectations of the CCTL

During pre-evaluation, the sponsor can expect that the CCTL will:

a) be knowledgeable of the CC, the CEM, CCEVS procedures and (as required in order to accomplish the evaluation) the specific technology being evaluated;

b) notify the Validation Body of the intent to perform an evaluation under the scheme;

c) coordinate with the Validation Body to obtain Validation Body approval of the evaluation under scheme oversight, achieving an agreed to evaluation work plan and schedule; and

d) provide a conduit for information flow between the sponsor and the Validation Body.

4.1.11 Sponsor's Expectations of the Validation Body

During pre-evaluation, the sponsor can expect that the Validation Body will:

a) coordinate with the CCTL to achieve an agreed to evaluation work plan and schedule; and

b) officially accept the PP or ST/TOE into evaluation for scheme validation and if unable to do so, provide to the CCTL and the sponsor a written rationale for a decision not to accept.

4.2 Evaluation

The *Evaluation* phase commences once the legal agreements are signed and ends just prior to the posting of the Validated Products List entry.

4.2.1 Sponsor's Responsibilities

While the security evaluation is in progress, it is the responsibility of the sponsor to:

a) inform the CCTL of any changes to the TOE which may affect the security evaluation;

b) answer any questions from the CCTL arising from the analysis of the ST, PP, or other evaluation deliverables;

c) provide the CCTL (and Validation Body, as required) with detailed proposals for resolving problems that arise during the course of evaluation;

d) provide the CCTL with a schedule for the delivery of all items necessary for the conduct of the evaluation as outlined in the deliverables list;

e) ensure the timely provision to the CCTL of identified deliverables for the evaluation including, as required by the ST:

    1) the TOE in its various representations, (e.g., architectural design, detailed design and implementation, source code);

    2) configuration data, defining all configurable options of the TOE which could affect security;

    3) evidence of security (e.g., justifications, conformance analyses, proofs and test materials);

    4) develop documentation describing configuration control, programming languages, compilers, and developer security;

5) operational documentation for delivery, configuration, start-up, and operation; and
6) user and administrative documentation.

f) provide access to an appropriate facility where the TOE can be installed and tested in the evaluated configuration;

g) provide general support to evaluators and validation personnel, including training and access to the developers staff for technical discussions about the product; and

h) hold evaluation progress reviews with the CCTL and Validation Body when required.

If the Sponsor wishes to have their product/system or PP posted on the NIAP CCEVS web site as "in evaluation", the sponsor must submit a letter or email to the CCEVS Director asking that it be posted accordingly. A copy of the request should also be sent to the CCEVS Deputy Director and the validator assigned to the project.

4.2.2 Sponsor's Expectations of CCTL During Evaluation

The CCTL is expected to:

a) conduct the evaluation in accordance with the requirements of the contract between the sponsor and the CCTL;
b) advise the sponsor of any unforeseen difficulties with the evaluation;
c) whenever feasible, provide the sponsor with the opportunity to correct deficiencies in the PP or the ST/TOE in lieu of evaluation failure;
d) coordinate with the Validation Body (validator) during the evaluation to ensure:
    1) on-going validator awareness of evaluation status; and
    2) timely validator awareness of evaluation problems and questions;
e) issue timely observation reports as required to the validator covering items such as, but not necessarily limited to:
    1) evaluation activities not covered, or not adequately covered, by the CEM; and
    2) technology specific evaluation issues;
f) respond to observation decisions from the Validation Body;
g) produce an Evaluation Technical Report (ETR) meeting all ETR requirements;

h) provide a conduit for information flow between the sponsor and the Validation Body;

i) be fully aware of all CC and CEM interpretations, and CCEVS policy/procedures impacting the evaluation; and

j) advise the sponsor on available means for increasing the efficiency of the evaluation (e.g., additional sponsor provided information that would result in reduced evaluator actions or reuse of existing evaluation evidence).

4.2.3 Sponsor's Expectations of Validator During Evaluation

The Validation Body (validator) is expected to:

a) coordinate with the CCTL to ensure:

   1) on-going validator awareness of evaluation status; and

   2) timely validator awareness of evaluation problems and questions;

b) issue timely observation decisions in response to CCTL generated observation reports;

c) ensure that all Validation Body oversight requirements are being met;

d) be knowledgeable of the CC, the CEM, CCEVS procedures and (as required in order to oversee the evaluation) the specific technology being evaluated;

e) clearly indicate to the sponsor and CCTL which CC or CEM interpretations are to be applied to this evaluation; and

f) provide the sponsor with Validation Body point of contact and the process for direct sponsor to scheme communications for purposes such as, but not necessarily limited to:

   1) requesting additional government involvement in the evaluation; and

   2) appealing a decision of the CCTL or validator.

4.2.4 Evaluation Specifics

4.2.4.1 PP Evaluation

The goal of a protection profile evaluation is to demonstrate that the profile is complete, consistent, and technically sound and, hence, suitable for use as a statement of requirements for one or more TOEs that may be evaluated against it. In addition to the PP, the sponsor may want to provide the CCTL any relevant documentation associated with the development of the PP.

4.2.4.2 ST/TOE Evaluation

The goal of an IT product/system evaluation is two-fold:

a) demonstrate that the ST is complete, consistent, and technically sound, meets any PP compliance claims and, hence, suitable for use as a statement of requirements for the TOE; and

b) demonstrate that the TOE complies with the requirements specified in the ST.

4.2.5 Complaints and Appeals

The Validation Body provides a process for addressing complaints and appeals that originate either internally or externally. The process applies, but is not limited to:

- CCEVS actions, decisions, approvals, or staff assignments,
- Validation Body customers and consumers,
- Internal quality system problems that may be detected by CCEVS staff members,
- CCTLs, candidate CCTLs, CCTL customers, or
- Unresolved issues that occur during PP or IT product/system evaluations.

The Director of the Validation Body is responsible for ensuring that all complaints and appeals are responded to promptly and that corrective action, if required, is implemented. For more details about the Complaint and Appeal process, refer to Scheme Publication #2, *NIAP Common Criteria Evaluation and Validation Scheme for IT Security -- Validation Body Standard Operating Procedures*, which can be found at http://niap.nist.gov/cc-scheme/GuidanceDocs.html.

4.3 Post-Evaluation

Post-evaluation commences with the issuance of the certificate and the publication of the Validated Products List entry.

4.3.1 Certificate Issuance

Upon completion of the evaluation, the CCTL will provide the Validator with an Evaluation Technical Report (ETR, as defined in the CEM), all evaluation Observation Reports and corresponding Observation Decisions, and a draft Validated Products List Entry Summary. After a review of all information, the Validator will produce a Validation Report and recommendation. The Validation Report and Validated Products List Entry Summary will concurrently be submitted to the sponsor and CCTL for accuracy and release approval.

Validators will provide a final recommendation to the CCEVS Technical Oversight Manager for concurrence and presentation to the Director of the Validation Body.

Using the final recommendation, the Director of the Validation Body will make the decision to either:

1) prepare a CC certificate for signature, issue a Validated Products List entry, and notify our CC partner schemes for mutual recognition; or

2) notify the CCTL and sponsor of the unsuccessful completion of the evaluation and the rationale for this decision.

Following the decision to issue a CC certificate for a product or PP, the Director of the Validation Body prepares the certificate and rationale for issuing the certificate and forwards them to NSA and NIST signatories. CC certificates are issued to product developers, sponsors, or PP developers on behalf of IT products and PPs that have been evaluated and validated against the CC according to the rules of the CCEVS. To be valid, the certificates must be signed by both the NIST and NSA signatories. The contents of a CC certificate are described in Scheme Publication #1, *NIAP Common Criteria Evaluation and Validation Scheme for IT Security -- Organization, Management and Concept of Operations,* Annex E.

The certificate applies only to the specific version and release of the PP or the IT product in its evaluated configuration. A sponsor of an evaluation shall only market an IT product or a PP as an evaluated product or an evaluated profile, respectively, on the basis of the validation report and accompanying Common Criteria certificate published by the Validation Body. The issuance of a certificate does not imply endorsement of an IT product or PP by NIST, NSA, or any other agency of the U.S. Government.

The Validation Body will monitor the use of CC certificates for each CCEVS validated product to verify that all rules associated with the use of the certificates are being adhered to. The holder of a certificate can use the certificate for any purpose as long as such use does not misrepresent or violate the intent or rules of the CCEVS or CCRA. The rules governing the use of CC certificates can be found in Scheme Publication #2, *NIAP Common Criteria Evaluation and Validation Scheme for IT Security -- Validation Body Standard Operating Procedures*.

The Validation Body notifies the CCRA partners of the certificate issuance and are provided with the same information that is published in the Validated Products List. The Validated Products List is a summary of certificate information for all validated products. Validated Products are products or PPs that have received a CC certificate.

4.3.2 Evaluation Records Management

All records pertaining to an evaluation will be kept by the Scheme for at least five years after the completion of the evaluation. This includes all records and other papers produced in connection with each evaluation. After the archive period has expired, all non-proprietary records supporting an evaluation will be destroyed. All proprietary information stored on behalf of a sponsor will be returned to the entity unless the entity gives the Validation Body other directions.

4.3.3 Sponsor Responsibilities Pertaining to Evaluation Completion

Upon completion of the security evaluation, it is the responsibility of the sponsor:

a) to reach agreement with the Validation Body that the validation report fairly and accurately represents the PP/ST and outcome of the evaluation;

b) to accept the conclusions in the validation report;

c) to inform the Validation Body of any factors that would invalidate or change the validation report;

d) to reproduce and distribute the validation report only in its entirety;

e) to advertise and market an IT product or PP as a validated product or profile only on the basis of a valid Common Criteria certificate;

f) to provide the Validation Body with reference material uniquely identifying the evaluated version of the TOE;

g) to retain archival material returned from the CCTL for a period of five years;

h) to ensure maintenance of the Common Criteria certificate by complying with the change control requirements specified in the ST, evaluation technical report, or validation report for proposed changes to the TOE; and

i) to retain all evaluation deliverable change information and related test evidence for potential use in future evaluations.

4.3.4 Common Criteria Certificate Maintenance

The CCEVS provides an opportunity for sponsors of security evaluations to maximize previous evaluation results and to cost-effectively continue to participate in the evaluation and validation processes over time. Procedures for the maintenance of Common Criteria certificates, (e.g., in conjunction with extensions to later releases or versions of the IT product or PP), are governed by the Common Criteria Certificate Maintenance Program (CMP).

A sponsor, anticipating the need for re-evaluation, may wish to consider a certificate maintenance approach during the early stage of the initial evaluation in order to minimize future evaluation activities. Sponsor coordination with a CCTL may be required in order to take re-evaluation or certificate maintenance requirements into account when performing the initial evaluation of the IT product/system.

Assurance maintenance concepts are primarily applicable to IT product evaluations, though many of those same concepts can be applied to PP evaluations.

Certificates are only valid for a specific version of a TOE. However, most IT products that have been evaluated, continue to change over time as the products evolve and are enhanced with new features and capabilities. These changes are usually outside the scope of the current certificate issued by the Validation Body. The CMP provides a means of establishing confidence that the assurance in a TOE is maintained without always requiring a formal re-evaluation. The sponsor, under the CMP, is therefore able to maintain their TOE without incurring the costs associated with re-evaluating each change and at the same time, minimize the cost of future re-evaluation. In addition, the CMP has been designed to ensure that mutual recognition of certificates issued by the Validation Body is not jeopardized.

Specific details of the CMP employed within the scheme are provided in Scheme Document #6 *NIAP Common Criteria Evaluation and Validation Scheme for Information Technology Security—Certificate Maintenance Program*.

Annex A. Demonstrating Conformance

Sponsors of security evaluations can participate in many different types of activities when considering the issue of IT product or PP conformance to Common Criteria requirements. While all of these activities are recognized as legitimate for certain constituencies or communities of interest, some are outside the scope of the Common Criteria Scheme as described in this document and will not result in the issuance of a Common Criteria certificate. The different approaches to conformance (both within the scope of the scheme and outside the scope of the scheme) are summarized below and illustrated pictorially in Figure A-1.

Third Party Evaluation and U.S. Government Validation
(NIAP Common Criteria Scheme)

A sponsor can submit an IT product or PP to a NVLAP-accredited CCTL for a formal, independent, third party evaluation with government-sponsored oversight and validation. The sponsor asserts conformance to Common Criteria requirements based on the results of the security evaluation conducted by the CCTL and the validation process conducted by the NIAP Validation Body. A final report is published by the NIAP Validation Body and a Common Criteria certificate is issued for the product or profile after successfully completing evaluation and validation. Following validation, the IT product or PP is placed on the NIAP Validated Products List. Sponsors employing this approach will receive the benefits that accrue from the CCRA.

Third Party Evaluation and Private Sector Validation
(Outside Scope of NIAP Common Criteria Scheme)

A sponsor can submit an IT product or PP to a NVLAP-accredited CCTL for a formal, independent, third party evaluation with private sector oversight and validation. This approach will likely be used by sponsors who wish to have their products or profiles evaluated by an accredited testing laboratory but are not interested in participating in a government-sponsored validation process. The sponsor is, however, interested in submitting the results of the security evaluation to a specific private sector Validation Body operating on behalf of a particular constituency or community of interest; e.g., a banking association, a health care association, an industry consortium, or a trade association. A certificate may be issued by the Validation Body providing recognition within that particular constituency or community of interest. There may also be validated products lists maintained by these private sector validation bodies as a service to their respective communities. Sponsors employing this approach will not be able to have their evaluated IT products or PPs placed on the NIAP Validated Products List and will not receive the benefits that accrue from the CCRA.

Third Party Evaluation without Validation

(Outside Scope of NIAP Common Criteria Scheme)

A sponsor can submit an IT product or PP to a NVLAP-accredited CCTL for a formal, independent, third party evaluation without validation. The sponsor asserts conformance to Common Criteria requirements based solely on the results of the security evaluation as articulated in the evaluation technical report produced by the CCTL. Conformance is demonstrated by third party evaluation without government or private sector validation, providing a degree of assurance that may be acceptable to certain constituencies or consumers. However, it is again outside the scope of the scheme. Sponsors employing this approach will not be able to have their evaluated IT products/systems or protection profiles placed on the NIAP Validated Products List and will not receive the benefits that accrue from the CCRA.

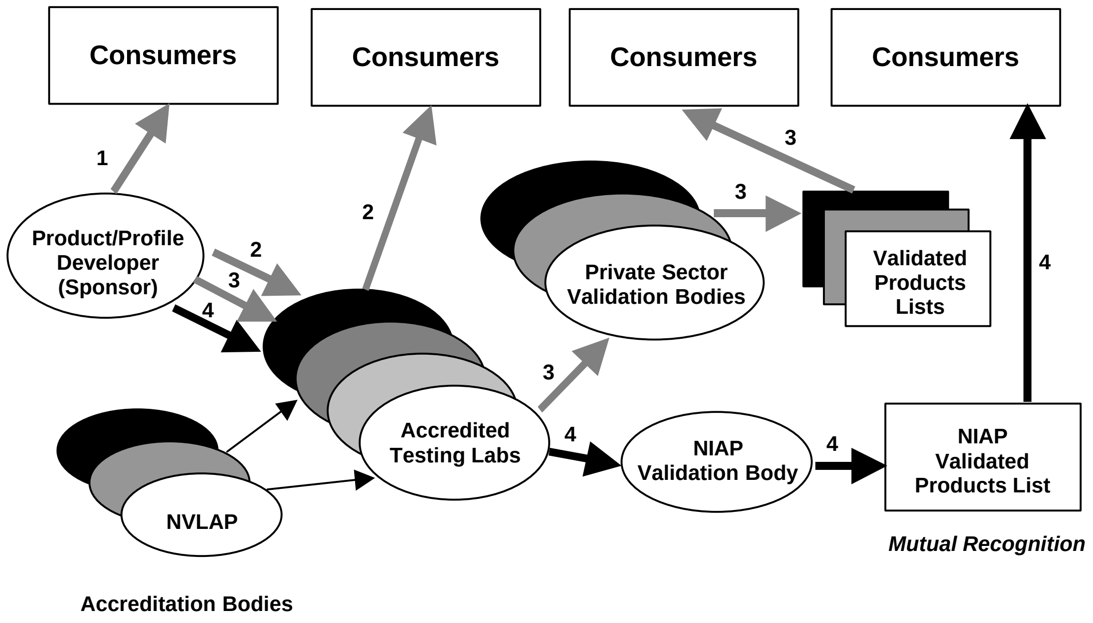
Developer Self-Declaration

(Outside Scope of NIAP Common Criteria Scheme)

An IT product or PP developer can assert that their product or profile has been built to meet the requirements articulated in the Common Criteria. The developer sells the product or profile to the consumer neither without the intervention of third party security testing or evaluation activity nor of a Validation Body. This approach provides a degree of assurance that may be acceptable to certain constituencies or consumers. Specifically, even without third-party evaluation and validation, the use the Common Criteria construct (security target) incorporating common language to express security claims and requirements meeting these claims is a significant improvement over current, typical presentations from vendor to customer. Developer self-declaration of conformity is outside the scope of the scheme. Developers employing this approach will not be able to have their IT products or PPs placed on the NIAP Validated Products List and will not receive the benefits that accrue from the CCRA.

Figure A-1 illustrates the different types of Common Criteria conformance activities and approaches that IT product and PP developers can take according to consumer needs.

Figure A-1 CC Conformance Approaches



Approach 1: Developer or vendor self-declaration of conformity. (Outside scheme)
Approach 2: Conformance demonstrated by third party evaluation only. (Outside scheme)
Approach 3: Conformance demonstrated by third party evaluation and private sector validation. (Outside scheme)
Approach 4: Conformance demonstrated by third party evaluation and U.S. Government validation.

Figure A-1. Approaches and Activities for Achieving Common Criteria Conformance

Annex B. Related Documents and Web sites

Following is a reference list of CCEVS related documents and web sites.

1. **NIAP Common Criteria Evaluation and Validation (CCEVS) Homepage**
   http://niap.nist.gov/cc-scheme/index.html

2. **NIAP CCEVS Educational Courses**
   http://www.niap.nist.gov/event.html#Classes

3. **NIAP CCEVS Guidance Documents**
   http://niap.nist.gov/cc-scheme/GuidanceDocs.html

4. **Common Criteria Interpretation Management Board (CCIMB)**
   http://www.commoncriteria.org

5. **CCEVS Interpretations**
   http://niap.nist.gov/cc-scheme/

6. **NIAP Validated Products List**
   http://niap.nist.gov/cc-scheme/ValidatedProducts.html

7. **Common Criteria Version 2: An Introduction (19-page brochure providing a summary of the principal feature of the Common Criteria)**
   http://csrc.nist.gov/cc/info/ccbrochure.pdf

8. **Common Criteria Version 2.1 / ISO IS 15408**
   http://csrc.nist.gov/cc/ccv20/ccv2list.htm

9. **Common Evaluation Methodology (CEM) Documents**
   http://csrc.nist.gov/cc/cem/cemlist.htm

10. **Protection Profile Registry**
    http://csrc.nist.gov/cc/pp/pplist.htm

11. **CC Toolbox (integrated tool set to aid systems developers and profile authors to generate PPs and STs)**
    http://niap.nist.gov/secrequire.htmlCCToolbox

12. **NIAP CCEVS Approved (NVLAP Accredited) Common Criteria Testing Laboratories (CCTL)**
    http://niap.nist.gov/cc-scheme/TestingLabs.html

13. **Guidance for COTS Security Protection Profiles (CSPP, NISTIR 6462)**
    http://csrc.nist.gov/publications/nistir/index.html

Annex C. Sample Non-Disclosure Agreement

Sample EVALUATION ACCEPTANCE AND NON-DISCLOSURE AGREEMENT (See http://niap.nist.gov/cc-scheme for the latest official electronic copy):

THIS AGREEMENT, made this ______day of ____________________, 20___, is between ________________________, hereinafter referred to as Sponsor, ________ __________________, hereinafter referred to as CCTL, and the National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme, hereinafter referred to as CCEVS.

WHEREAS, the Sponsor, CCTL, and CCEVS desire to enter into evaluation and discussions concerning a product described as _________________________ submitted to CCEVS. To enable the CCEVS to conduct the necessary government oversight of the evaluation of the product by the CCTL, it may be necessary for the CCTL and/or Sponsor to disclose to the CCEVS certain information which is proprietary to the Sponsor and/or CCTL ("Proprietary Information").

NOW THEREFORE, to protect such Proprietary Information the Sponsor, CCTL, and CCEVS agree as follows:

1. Proprietary Information may include, without limitation, trade secrets, business plans, financial data, technical data, and other items pertaining to the above proposed product as be necessary or desirable to conduct the evaluation.

2. To be protected hereunder, all Proprietary Information provided to the CCEVS must be clearly identified and properly marked by the Sponsor and/or CCTL so that such information can be protected by the CCEVS to the full extent authorized by law.

3. To the extent permitted by law, all Proprietary Information provided under this Agreement will be held in strict confidence and only used as necessary to perform the evaluation and evaluation oversight. If required, the CCEVS will actively solicit the Sponsor's and CCTL's assistance in establishing supportable bases for protecting such Proprietary Information in response to Freedom of Information Act requests. CCEVS will not transfer or assign any Proprietary Information outside of CCEVS without prior written consent of the Sponsor and/or CCTL as appropriate.

4. No grant, ownership, license, or right other than as specified herein, is transferred hereby. No modification of any kind of the Source Code or any other Proprietary Information is permitted under this Agreement without the prior written permission of the Sponsor. Specifically, CCEVS agrees not to alter,

remove, or otherwise disturb any notices of Intellectual or proprietary rights, including without limitation copyright. The Sponsor and/or CCTL is specifically not responsible for use of any Sponsor or CCTL Proprietary Information for other than an evaluation. Except as necessary to conduct an evaluation, reverse engineering, decompilation and other source code derivations of any object code is specifically prohibited.

5. CCEVS shall not be liable for any unauthorized disclosure or use of Proprietary Information if it:

(a) is presently known or hereafter becomes known to the public by other than breach of the CCEVS' obligations hereunder, or
(b) is known to the CCEVS without restriction prior to the time disclosure of it by the Sponsor or CCTL, or
(c) is subsequently and independently developed by the CCEVS without resort to the Sponsor's or CCTL's disclosure, or
(d) is independently and rightfully acquired by the CCEVS from another source without restriction on disclosure or use, or
(e) is identified by the Sponsor or CCTL to be no longer subject to this Agreement.

6. The receipt of this information by the CCEVS for the purpose of performing government oversight of the evaluation shall not be construed in any way as a commitment to the Sponsor or CCTL for any future procurement of any equipment or other items of supply or service sold by the Sponsor or CCTL nor in any way be permitted to provide a basis or argument for sole source procurement that might otherwise prevent free and full competition.

7. It is mutually understood and agreed that the evaluation oversight will be conducted by validators for the CCEVS. It is further understood and agreed that the CCEVS's validators may include authorized agents who are under contract with the CCEVS and who are bound to abide by all terms, conditions, and references of this Agreement.

8. Any report or other information provided by the CCEVS to the Sponsor and/or CCTL arising out of or as a result of this Agreement or the evaluation is not to be construed as an endorsement of the Sponsor's or CCTL's goods and/or services and the Sponsor and/or CCTL will not, by advertising or otherwise, claim or imply the existence of a CCEVS endorsement of its goods and/or services covered by this Agreement.

9. This Agreement shall be governed by, and construed in accordance with, federal statutes and regulations, notwithstanding any State conflict of law statutes, practices or rules of construction. To the extent that no federal law applies, the law of the State of ______________________shall apply without giving effect to its conflict of law provisions.

10. This Agreement shall be effective from the date which first appears in this Agreement until terminated in writing by either party with or without cause. The CCEVS's obligation to protect Proprietary Information shall continue for a period of five (5) years following disclosure of such information to the CCEVS. Within ten (10) days of termination of this Agreement, CCEVS shall return all originals of the Source Code and any other Proprietary Information of the Sponsor or CCTL which has been fixed in any tangible means of expression, and any copies thereof. It is further understood and agreed that for security reasons CCEVS will not return to the Sponsor or CCTL any software or magnetic media which has been installed on a CCEVS system and the CCEVS will destroy said software upon completion of the Agreement. Any documentation provided with the software will be returned to the Sponsor or CCTL upon termination as appropriate.

11. Neither failure to require performance, nor waiver of a breach, of any provision of this Agreement constitutes any waiver of a party's right to subsequently require full performance of that provision.

12. No promise of payment is made herein and this Agreement constitutes the total obligation of the parties. This Agreement is the complete and exclusive statement of the parties on these specific subjects, and supersedes all prior written or oral agreements, proposals, and understandings relating thereto.

13. This Agreement may only be modified by a writing signed by an officer of the party to be bound. If any court of competent jurisdiction determines that any provision of this Agreement is invalid, the remainder of the Agreement will continue in full force and effect, and the invalid provision shall be restated to most nearly give effect to its stated intent.

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

BY: ______________________________
TITLE: ____________________________
DATE: ____________________________

SPONSOR'S NAME
Address
City, State

BY:__________________________
TITLE:__________________________
DATE:__________________________

CCTL'S NAME
Address
City, State

BY: _____________________________
TITLE: ____________________________
DATE: ____________________________

Annex D. Acronyms

CC (CCITSE)	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretation Management Board
CCRA	Agreement on the Recognition of Common Criteria Certificates in the field of IT Security
CCTL	Common Criteria Testing Laboratory
CEM	Common Methodology for Information Technology Security Evaluation
CMP	Certificate Maintenance Program
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FAQ	Frequently Asked Questions
ISO	International Organization for Standardization
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
VPL	Validated Products List